Claims

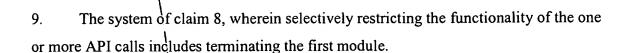
Express

What is claimed is:

A system for regulating access to a platform comprising:

a component for analyzing a first module and an application environment associated with the first module and determining a level of access to the platform, and applying a trust level to the first module corresponding to the determined level of access.

- 2. The system of claim 1, the component for analyzing the first module providing for inheritance of the trust level.
- 3. The system of claim 1, the component for analyzing the first module providing for marking the first module with at least one of states: (1) fully trusted, (2) run restricted, and (3) fail to load.
- 4. The system of claim 1, wherein the component is stored in a Read Only Memory (ROM) in the platform.
- 5. The system of claim 1, wherein the component is part of an operating system.
- 6. The system of claim 1, wherein the trust level is utilized to regulate access to the platform of one or more second modules called by the first module.
- 7. The system of claim 1, wherein the functionality of one or more Application Programming Interface (API) calls, when called by the first module, are selectively restricted.
- 8. The system of claim 7, wherein selectively restricting the functionality of the one or more API calls includes restricting the functionality to read functions.



Express

- 10. A system for regulating access to a platform, comprising:

 means for determining a trust level for a first module; and

 means for applying the trust level to the first module to regulate access to the

 platform.
- 11. The system of claim 10 further comprising means for applying the trust level to one or more second/modules called by the first module.
- 12. A method for regulating access to a platform, comprising the steps of:

 determining a trust level for a first module; and
 applying the trust level to the first module to regulate access to the platform.
- 13. The method of claim 12 wherein determining the trust level for the first module further comprises the step of marking the first module with at least one of states: (1) fully trusted, (2) run restricted, and (3) fail to load.
- 14. The method of claim 12 wherein determining the trust level for the first module further comprises transmitting the first module to a verification program.
- 15. The method of claim 12 wherein regulating access to the platform further comprises selectively aborting calls made to one or more APIs.
- 16. The method of claim 12 wherein regulating access to the platform further comprises selectively terminating the first module.
- 17. The method of claim 12 wherein the program for determining the trust level for the first module is stored in a ROM in the platform.



- 18. The method of claim 12 wherein the logic for applying the trust level to regulate access to the platform is stored in a ROM in the platform.
- 19. The method of claim 12 wherein the trust level may be inherited.
- 20. The method of claim 12 wherein the trust level may be applied to one or more second modules called by the first module.